

# **USER AUTHENTICATION SYSTEM, AND METHOD THEREFOR**

**Publication number:** JP2002222170 (A)

**Publication date:** 2002-08-09

**Inventor(s):** OHARA TAKAO; ITO YUICHIRO; TERUI AKIO; OKI HIROSHI; TAKAISHI ATSUYA +

**Applicant(s):** NINTENDO CO LTD; KYOCERA COMM SYSTEMS CO LTD +

**Classification:**

**- International:** G06F15/00; G06F21/20; H04L9/32; G06F15/00; G06F21/20; H04L9/32; (IPC1-7): G06F15/00, H04L9/32

**- European:**

**Application number:** JP20010019312 20010126

**Priority number(s):** JP20010019312 20010126

**Abstract of JP 2002222170 (A)**

**PROBLEM TO BE SOLVED:** To conduct a user authentication with high reliability even for an Internet terminal of low level specification. **SOLUTION:** An authentication server 10 stores a table wherein the first identification information is made preliminarily to correspond to the second identification information. A key prepared optionally by the server 10 is received in a hand-held terminal 100. Irreversible change information of information including the key and the second identification information is computed thereafter to transmit information added to the irreversible change information with the key and the first identification information, as an authentication code. The second identification information is acquired in an authentication server 10 side based on the first identification information in the received authentication code, referring to the table. Then, irreversible change information of information including the second identification information and the key in the received authentication code is computed. The user is authenticated when the resulting irreversible change information is consistent with the irreversible change information in the received authentication code.



Data supplied from the **espacenet** database — Worldwide

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-222170

(P2002-222170A)

(43) 公開日 平成14年8月9日(2002.8.9)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード <sup>*</sup> (参考)	
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B	5 B 0 8 5
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 A	5 J 1 0 4
			6 7 5 A	

審査請求 有 請求項の数13 ○L (全 16 頁)

(21) 出願番号 特願2001-19312(P2001-19312)

(22) 出願日 平成13年1月26日(2001.1.26)

(71) 出願人 000233778

任天堂株式会社

京都府京都市南区上鳥羽錦立町11番地1

(71) 出願人 596100812

京セラコミュニケーションシステム株式会社  
京都府京都市伏見区竹田島羽殿町6番地

(72) 発明者 大原 貴夫

京都府京都市南区上鳥羽錦立町11番地1

任天堂株式会社内

(74) 代理人 100092956

弁理士 古谷 栄男 (外2名)

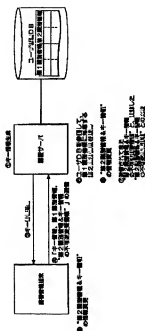
最終頁に続く

(54) 【発明の名称】 ユーザ認証システム及びその方法

## (57) 【要約】

【課題】 低スペックのインターネット端末に対して、信頼性の高いユーザ認証を行うことができるユーザ認証システム及びその方法を提供する。

【解決手段】 認証サーバ10は、あらかじめ第1識別情報と第2識別情報を対応づけたテーブルを記憶している。携帯情報端末100側では、認証サーバ10が任意に作成するキーを受信する。次に、このキーと第2識別情報とを含めた情報の不可逆変更情報を演算し、この不可逆変更情報に、キーと、第1識別情報と、を付加したものを認証コードとして送信する。認証サーバ10側では、受信した認証コード中の第1識別情報に基づき、テーブルを参照して第2識別情報を取得する。次に、この第2識別情報と、受信した認証コード中のキーとを含めた情報の不可逆変更情報を演算する。そして、得られた不可逆変更情報と、受信した認証コード中の不可逆変更情報とが一致すれば、ユーザ認証をする。



## 【特許請求の範囲】

【請求項1】 ユーザ端末と、前記ユーザ端末とネットワークで接続される認証装置と、を備えており、前記認証装置は、キー情報と前記ユーザ端末から送信される認証用情報とに基づいて前記ユーザ端末のユーザの認証を行うユーザ認証システムであって、前記ユーザ端末は、前記認証装置にアクセスして前記キー情報を受信するキー情報受信手段、前記ユーザ端末のユーザを識別するための第1識別情報と第2識別情報とを入力する識別情報入力手段、前記第2識別情報と前記キー情報とを含めた情報に対して情報変更を行うことにより、この情報変更後に生成される情報単独では前記情報変更のアルゴリズムを利用しても前記情報変更前の情報の再現ができない、不可逆変更情報を生成する不可逆変更情報生成手段、前記キー情報と、前記第1識別情報と、前記不可逆変更情報と、を含んだ情報を前記認証用情報として生成する認証用情報生成手段、前記認証用情報を送信する認証用情報送信手段、を備えており、前記認証装置は、前記第1識別情報と前記第2識別情報とを関連づけて記憶する識別情報記憶手段、前記ユーザ端末からのアクセスがあるごとに任意の前記キー情報を送信するキー情報送信手段、前記認証用情報を受信する認証用情報受信手段、前記認証用情報に含まれる前記キー情報を取得するキー情報取得手段、前記認証用情報に含まれる前記第1識別情報に基づいて前記識別情報記憶手段を検索することにより前記第2識別情報を取得する第2識別情報取得手段、前記第2識別情報取得手段が取得した第2識別情報と前記キー情報取得手段が取得したキー情報とを含めた情報に対して前記情報変更を行うことにより確認用不可逆変更情報を生成する確認用不可逆変更情報生成手段、前記認証用情報の不可逆変更情報と前記確認用不可逆変更情報とに基づいて前記ユーザ端末のユーザを認証するユーザ認証手段、を備えたことを特徴とするユーザ認証システム。

【請求項2】 キー情報と認証用情報とに基づいてユーザの認証がなされることとされるユーザ端末であって、前記キー情報を受信するキー情報受信手段、前記ユーザ端末のユーザを識別するための第1識別情報と第2識別情報とを入力する識別情報入力手段、前記第2識別情報と前記キー情報とを含めた情報に対して情報変更を行うことにより、この情報変更後に生成される情報単独では前記情報変更のアルゴリズムを利用しても前記情報変更前の情報の再現ができない、不可逆

変更情報を生成する不可逆変更情報生成手段、前記キー情報と、前記第1識別情報と、前記不可逆変更情報と、を含んだ情報を前記認証用情報として生成する認証用情報生成手段、前記認証用情報を送信する認証用情報送信手段、を備えたことを特徴とするユーザ端末、【請求項3】 キー情報と認証用情報とに基づいてユーザ端末のユーザの認証を行う認証装置であって、前記認証用情報は、前記キー情報と、前記ユーザ端末のユーザを識別するための第1識別情報と、前記ユーザ端末のユーザを識別するための第2識別情報と前記キー情報とを含めた情報に対して情報変更を行うことにより、この情報変更後に生成される情報単独では前記情報変更のアルゴリズムを利用しても前記情報変更前の情報の再現ができない、不可逆変更情報と、を含んだ情報とされており、前記認証装置は、前記第1識別情報と前記第2識別情報とを関連づけて記憶する識別情報記憶手段、前記ユーザ端末からのアクセスがあるごとに任意の前記キー情報を送信するキー情報送信手段、前記認証用情報を受信する認証用情報受信手段、前記認証用情報に含まれる前記キー情報を取得するキー情報取得手段、前記認証用情報に含まれる前記第1識別情報に基づいて前記識別情報記憶手段を検索することにより前記第2識別情報を取得する第2識別情報取得手段、前記第2識別情報取得手段が取得した第2識別情報と、前記キー情報取得手段が取得したキー情報とを含めた情報に対して前記情報変更を行って確認用不可逆変更情報を生成する確認用不可逆変更情報生成手段、前記認証用情報の不可逆変更情報と前記確認用不可逆変更情報とに基づいて前記ユーザ端末のユーザを認証するユーザ認証手段、を備えたことを特徴とする認証装置、【請求項4】 キー情報と認証用情報とに基づいてユーザの認証がなされることとされるユーザ端末を機能させるためのプログラムを記録した記録媒体であって、前記記録媒体は、前記ユーザ端末を以て、前記キー情報を受信するキー情報受信手段、前記ユーザ端末のユーザを識別するための第1識別情報と第2識別情報とを入力する識別情報入力手段、前記第2識別情報と前記キー情報とを含めた情報に対して情報変更を行うことにより、この情報変更後に生成される情報単独では前記情報変更のアルゴリズムを利用しても前記情報変更前の情報の再現ができない、不可逆変更情報を生成する不可逆変更情報生成手段、前記キー情報と、前記第1識別情報と、前記不可逆変更情報と、を含んだ情報を前記認証用情報として生成する認証用情報生成手段、

前記認証用情報を送信する認証用情報送信手段、  
を備えたユーザ端末として機能させるためのプログラム  
を記録した記録媒体。

【請求項5】 キー情報と認証用情報とに基づいてユーザ  
端末のユーザの認証を行う認証装置を機能させるための  
プログラムを記録した記録媒体であって、

前記認証用情報は、前記キー情報と、前記ユーザ端末の  
ユーザを識別するための第1識別情報と、前記ユーザ端  
末のユーザを識別するための第2識別情報と前記キー情  
報とを含めた情報に対して情報変更を行うことにより、  
この情報変更後に生成される情報単独では前記情報変更  
のアルゴリズムを利用して前記情報変更前の情報の再  
現ができない、不可逆変更情報と、を含んだ情報とされ  
ており、

前記記録媒体は、前記認証装置を以下の、  
前記ユーザ端末からのアクセスがあることに任意の前記  
キー情報を送信するキー情報送信手段、

前記認証用情報を受信する認証用情報受信手段、  
前記認証用情報に含まれる前記キー情報を取得するキー  
情報取得手段、

前記認証用情報に含まれる前記第1識別情報に基づい  
て、あらかじめ前記第1識別情報に対応づけて記憶され  
た前記第2識別情報を取得する第2識別情報取得手段、  
前記第2識別情報取得手段が取得した第2識別情報と前  
記キー情報取得手段が取得したキー情報とを含めた情報  
に対して前記情報変更を行うことにより確認用不可逆変  
更情報を生成する確認用不可逆変更情報生成手段、

前記認証用情報の不可逆変更情報と前記確認用不可逆変  
更情報とに基づいて前記ユーザ端末のユーザを認証する  
ユーザ認証手段、

を備えた認証装置として機能させるためのプログラムを  
記録した記録媒体。

【請求項6】 キー情報と認証用情報とに基づいてユーザ  
の認証がなされることとされるユーザ端末を機能させる  
ためのプログラムであって、

前記プログラムは、前記ユーザ端末を以下の、  
前記キー情報を受信するキー情報受信手段、

前記ユーザ端末のユーザを識別するための第1識別情報  
と第2識別情報とを入力する識別情報入力手段、

前記第2識別情報と前記キー情報とを含めた情報に対し  
て情報変更を行うことにより、この情報変更後に生成さ  
れる情報単独では前記情報変更のアルゴリズムを利用し  
ても前記情報変更前の情報の再現ができない、不可逆変  
更情報を生成する不可逆変更情報生成手段、

前記キー情報と、前記第1識別情報と、前記不可逆変  
更情報と、を含んだ情報を前記認証用情報として生成する  
確認用情報生成手段、

前記認証用情報を送信する認証用情報送信手段、  
を備えたユーザ端末として機能させるためのプログラ  
ム。

【請求項7】 キー情報と認証用情報とに基づいてユーザ  
端末のユーザの認証を行う認証装置を機能させるための  
プログラムであって、

前記認証用情報は、前記キー情報と、前記ユーザ端  
末のユーザを識別するための第1識別情報と、前記ユーザ  
末のユーザを識別するための第2識別情報と前記キー情  
報とを含めた情報に対して情報変更を行うことにより、  
この情報変更後に生成される情報単独では前記情報変更  
のアルゴリズムを利用して前記情報変更前の情報の再  
現ができない、不可逆変更情報と、を含んだ情報とされ  
ており、

前記プログラムは、前記認証装置を以下の、  
前記ユーザ端末からのアクセスがあることに任意の前記  
キー情報を送信するキー情報送信手段、

前記認証用情報を受信する認証用情報受信手段、  
前記認証用情報に含まれる前記キー情報を取得するキー  
情報取得手段、

前記認証用情報に含まれる前記第1識別情報に基づい  
て、あらかじめ前記第1識別情報に対応づけて記憶され  
た前記第2識別情報を取得する第2識別情報取得手段、  
前記第2識別情報取得手段が取得した第2識別情報と前  
記キー情報取得手段が取得したキー情報とを含めた情報  
に対して前記情報変更を行うことにより確認用不可逆変  
更情報を生成する確認用不可逆変更情報生成手段、  
前記認証用情報の不可逆変更情報と前記確認用不可逆変  
更情報とに基づいて前記ユーザ端末のユーザを認証する  
ユーザ認証手段、

を備えた認証装置として機能させるためのプログラム。

【請求項8】 請求項1～7のいずれかにおいて、  
前記認証用情報に含まれるキー情報は、  
前記キー情報の一部分であるキー部分情報とされてお  
り、

前記認証装置は、さらに、  
前記キー情報送信手段が送信するキー情報と、このキー  
情報の前記キー部分情報とを関連づけて記憶するキー情  
報記憶手段、を備えており、

前記キー情報取得手段は、  
前記認証用情報に含まれる前記キー部分情報に基づいて  
前記キー情報記憶手段を検索することにより前記キー情  
報を取得することを特徴とするもの。

【請求項9】 請求項1～8のいずれかにおいて、  
前記ユーザ端末の認証用情報生成手段は、さらに、  
前記キー情報と、前記第1識別情報を暗号化したもの  
と、前記不可逆変更情報を暗号化したものと、を含んだ  
情報を、前記認証用情報として生成することと特徴とし  
ており、

前記認証装置は、さらに、  
前記認証用情報に含まれる前記第1識別情報を暗号化し  
たものと、前記不可逆変更情報を暗号化したものと、を  
それぞれ解読して、前記第1識別情報と前記不可逆変

情報とを得る暗号解読手段、

を備えたことを特徴とするもの。

【請求項10】請求項1～9のいずれかにおいて、

前記不可逆変更情報生成手段は、

前記第2識別情報と前記キー情報とを含めた情報に対するハッシュ値を演算することにより前記不可逆変更情報を生成することを特徴とするもの。

【請求項11】ネットワークを介して接続された認証装置を用いてユーザ端末のユーザの認証を行うユーザ認証方法であって、

前記ユーザ端末のユーザを識別するための第1識別情報と第2識別情報とをあらかじめ認証装置に記憶しておき、

認証装置は、前記ユーザ端末に対してキー情報を配布し、

前記ユーザ端末は、前記第2識別情報と前記キー情報とを含めた情報に対して情報変更を行うことにより、変更情報を生成し、

認証装置は、前記ユーザ端末から、前記キー情報と、前記第1識別情報と、前記変更情報と、を含んだ認証用情報を取得し、第2識別情報とキー情報とを含めた情報に対して前記情報変更を行うことにより確認用変更情報を生成し、前記認証用情報の変更情報と前記確認用変更情報とに基づいて前記ユーザ端末のユーザを認証する、ことを特徴とするユーザ認証方法。

【請求項12】互いに通信可能に接続された認証装置とユーザ端末とを用いてユーザの認証を行うユーザ認証方法であって、

前記ユーザ端末のユーザを識別するためのユーザ識別情報をあらかじめ認証装置に記憶しておき、

ユーザ端末は、認証装置から通信を介して取得したキー情報を用いて、ユーザ端末側で取得したユーザ識別情報に対して不可逆的な情報変更を行って、当該不可逆変更情報を通信によって認証装置に送信し、

認証装置は、予め記憶しているユーザ識別情報に対して、キー情報を用いて、ユーザ端末が行ったと同じ不可逆的な情報変更を行って、確認用変更情報を生成し、送信されてきた不可逆変更情報と確認用不可逆情報とに基づいて前記ユーザ端末のユーザを認証する、ことを特徴とするユーザ認証方法。

【請求項13】ユーザ端末と認証装置との間でユーザ認証のための情報を交換する情報交換方法であって、ユーザ端末からのアクセスがあるごとに、実質的に毎回異なるキー情報を認証装置からユーザ端末に送信し、当該キー情報を受けたユーザ端末は、キー情報およびユーザを識別するための識別情報を含む情報に対して不可逆的な変更を施した不可逆変更情報を認証装置に送信することを特徴とするユーザ認証のための情報交換方法。

【発明の詳細な説明】

【0001】

【発明の技術分野】この発明は、インターネット端末用のユーザ認証システム及びその方法に関するものであり、特に、低スペックインターネット端末のユーザ認証にも好適なものに関する。

【0002】

【従来の技術】現在、インターネットでユーザの認証を行うシステムの規格や手法が開発されており、そのようなシステムが様々な環境で利用されている。

【0003】

【発明が解決しようとする課題】しかしながら、現在利用されているユーザ認証システムの中で標準といわれているシステムは、あくまでも高性能な演算能力を持つクライアント機（パーソナルコンピュータ、ワークステーション等）に適した手法を利用するものである。そのような手法としては、例えば、SSL（Secure Sockets Layer）が利用されており、この手法では、プロトコルを2階層使用し、下位層でデータ配送等、上位層で認証、デジタル署名、暗号化等のネゴシエーションを行っている。このような手法では、データの配信だけでなく最初にネゴシエーションフェーズが入るので、そのための複雑な演算が必要となる。

【0004】したがって、十分な演算能力を持たないのが一般的な、携帯電話やネット対応時計等のようなインターネット端末に対しては、従来のユーザ認証システムを利用することは、実行時間等の観点から困難であった。

【0005】この発明は、上記のような問題に鑑みて、十分な演算能力を持たない低スペックのインターネット端末に対しても、信頼性の高いユーザ認証を行うことができるユーザ認証システム及びその方法を提供することを目的とする。

【0006】

【課題を解決するための手段および発明の効果】1）本発明のユーザ認証システムは、ユーザ端末と、前記ユーザ端末とネットワークで接続される認証装置と、を備えており、前記認証装置は、キー情報と前記ユーザ端末から送信される認証用情報とに基づいて前記ユーザ端末のユーザの認証を行うユーザ認証システムであって、前記ユーザ端末は、前記認証装置にアクセスして前記キー情報を受信するキー情報受信手段、前記ユーザ端末のユーザを識別するための第1識別情報と第2識別情報とを入力する識別情報入力手段、前記第2識別情報と前記キー情報とを含めた情報に対して情報変更を行うことにより、この情報変更後に生成される情報単独では前記情報変更のアルゴリズムを利用して前記情報変更前の情報の再現ができない、不可逆変更情報を生成する不可逆変更情報生成手段、前記キー情報と、前記第1識別情報と、前記不可逆変更情報と、を含んだ情報を前記認証用情報として生成する認証用情報生成手段、前記認証用情報を送信する認証用情報送信手段、を備えており、前記

認証装置は、前記第1識別情報と前記第2識別情報とを関連づけて記憶する識別情報記憶手段、前記ユーザ端末からのアクセスがあるごとに任意の前記キー情報を送信するキー情報送信手段、前記認証用情報を受信する認証用情報受信手段、前記認証用情報に含まれる前記キー情報を取得するキー情報取得手段、前記認証用情報に含まれる前記第1識別情報に基づいて前記識別情報記憶手段を検索することにより前記第2識別情報を取得する第2識別情報取得手段、前記第2識別情報取得手段が取得した第2識別情報と前記キー情報取得手段が取得したキー情報とを含めた情報に対して前記情報変更を行うことにより確認用不可逆変更情報を生成する確認用不可逆変更情報生成手段、前記確認用情報の不可逆変更情報と前記確認用不可逆変更情報とに基づいて前記ユーザ端末のユーザを認証するユーザ認証手段、を備えたことを特徴としている。

【0007】これにより、前記ユーザ端末は、前記第2識別情報を、この情報に対して前記情報変更を行うことにより、前記情報変更後に生成される情報単独では前記情報変更のアルゴリズムを利用して前記情報変更前の情報の再現ができない、不可逆変更情報としている。したがって、例えば、前記ユーザ端末の前記認証用情報送信手段が前記認証用情報を送信する際に第三者によって前記不可逆変更情報を不正に取得された場合でも、前記第2識別情報と前記キー情報とが再現されないため、前記ユーザ認証システムは、ユーザ認証を安全かつ適切に行うことができる。

【0008】また、前記第2識別情報は、前記認証装置が送信する任意の前記キー情報を含められて前記不可逆変更情報とされている。すなわち、同一の前記第2識別情報を用いていても、前記ユーザ端末は、ユーザ認証を受けるために前記認証装置にアクセスすることに異なる不可逆変更情報を生成する。したがって、第三者に前記不可逆変更情報を不正に取得された場合でも、その不可逆変更情報は別の認証では無効なものになるので、ユーザ認証の信頼性が確保される。

【0009】さらに、前記ユーザ端末の不可逆変更情報生成手段、及び、前記認証装置の確認用不可逆変更情報生成手段は、コンピュータによる簡単な情報変更を行うものである。したがって、前記ユーザ端末または前記認証装置として低い演算能力しか持たない低スペックの機器を採用した場合であっても、ユーザ認証を安全かつ適切に行うことができる。

【0010】また、前記認証装置の前記第2識別情報取得手段は、前記認証用情報に含まれる第1識別情報に基づいて前記識別情報記憶手段を検索することにより前記第2識別情報を取得する。したがって、前記認証装置は、前記確認用不可逆変更情報生成に必要となる前記第2識別情報を、迅速に取得することができるため、結果としてユーザ認証を迅速に行うことができる。

【0011】8）本発明のユーザ認証システムの前記認証用情報に含まれるキー情報は、前記キー情報の一部分であるキー部分情報とされており、前記認証装置は、さらに、前記キー情報送信手段が送信するキー情報と、このキー情報の前記キー部分情報とを関連づけて記憶するキー情報記憶手段、を備えており、前記キー情報取得手段は、前記認証用情報に含まれる前記キー部分情報に基づいて前記キー情報記憶手段を検索することにより前記キー情報を取得することを特徴としている。

【0012】これにより、例えば、前記認証装置のキー情報送信手段が前記ユーザ端末に前記キー情報を送信する際に第三者によって前記キー情報を不正に取得された場合でも、どのような規則で前記キー情報の一部分を前記キー部分情報としているかは特定されないため、第三者が前記キー部分情報を特定することは困難である。そして、前記認証装置の前記キー情報取得手段は、不適切なキー部分情報であれば前記キー情報を取得することができないため、ユーザ認証はされないことになる。したがって、前記ユーザ認証システムは、ユーザ認証をより安全かつ適切に行うことができる。

【0013】9）本発明のユーザ認証システムの前記ユーザ端末の認証用情報生成手段は、さらに、前記キー情報と、前記第1識別情報を暗号化したものと、前記不可逆変更情報を暗号化したものと、を含めた情報を、前記認証用情報として生成することを特徴としており、前記認証装置は、さらに、前記認証用情報に含まれる前記第1識別情報を暗号化したものと、前記不可逆変更情報を暗号化したものと、をそれぞれ解読して、前記第1識別情報と前記不可逆変更情報とを得る暗号解読手段、を備えたことを特徴としている。

【0014】これにより、前記認証用情報は、前記キー情報と、前記第1識別情報を暗号化したものと、前記不可逆変更情報を暗号化したものと、を含められて、前記ユーザ端末の認証用情報送信手段によって送信される。したがって、例えば、前記認証用情報を送信する際に第三者によって前記認証用情報を不正に取得された場合でも、第三者が前記第1識別情報と前記不可逆変更情報とを特定することは困難であるため、前記ユーザ認証システムは、ユーザ認証をより安全かつ適切に行うことができる。

【0015】10）本発明のユーザ認証システムの前記不可逆変更情報生成手段は、前記第2識別情報と前記キー情報とを含めた情報に対するハッシュ値を演算することにより前記不可逆変更情報を生成することを特徴としている。

【0016】これにより、前記ハッシュ値単独では、そのハッシュ値の演算アルゴリズムを知っていたとしても、前記第2識別情報と前記キー情報とを含めた元の情報を再現することはできない。また、前記第2識別情報と前記キー情報とを含めた元の情報が異なれば、同一の

ハッシュ値が得られる可能性は少ない。したがって、第三者によって前記ハッシュ値を不正に取得された場合でも、前記第2識別情報が取得されたり再現されることがないため、前記ユーザ認証システムは、ユーザ認証を安全かつ適切に行うことができる。

【0017】用語の定義について説明する。

【0018】この発明において、「不可逆変更情報生成手段」における「情報変更」とは、実施形態では、図6AステップS604でCPU102が行うハッシュ値の演算がこれに該当する。この「情報変更」は、情報変更後の情報のみでは、元の情報を再現することのできない処理を含む概念であり、ハッシュ関数（一方方向的関数、メッセージダイジェスト等も同様）によるもの、他、データの一部を所定の規則によって消去する手法も含まれる概念である。

【0019】「前記キー情報と、前記第1識別情報を暗号化したものと、前記不可逆変更情報を暗号化したものと、を含んだ情報」とは、実施形態では、図4ステップS516の認証コードがこれに該当する。なお、「前記第1識別情報を暗号化したものと、前記不可逆変更情報を暗号化したものと、を含む」概念については、前記第1識別情報と前記不可逆変更情報とを合わせた情報に対して暗号化した場合、及び、前記第1識別情報を暗号化した情報と前記不可逆変更情報を暗号化した情報とを合わせた場合、の両者を含む。

【0020】

【発明の実施の形態】1. システム概略

本発明の実施形態を図面に基いて説明する。本発明に係るユーザ認証システムとしての携帯情報端末用ユーザ認証システムは、図1に示すように、インターネット300に接続される携帯情報端末100と、認証サーバ10、Webサーバ200、とを備えている。認証サーバ10は、セッション管理データベース12と、ユーザ管理データベース14を備えている。

【0021】携帯情報端末100は、ユーザがインターネットに接続してサービスの提供を受けるためのものである。Webサーバ200は、インターネット上でユーザに対してサービスを提供するものである。認証サーバ10は、携帯情報端末100のユーザがWebサーバ200のサービスを利用する際にユーザ認証が必要となる場合に（例えば、課金発生時等）、ユーザ認証処理を行うものである。

【0022】2. ハードウェア構成

図2は、認証サーバ10のハードウェア構成の一例である。認証サーバ10は、CPU16、ハードディスク20、メモリ18、インターネット300に接続するための通信回路22を備えている。ハードディスク20には、セッション管理データベース12、ユーザ管理データベース14、ユーザ認証プログラムが記録されている。

【0023】Webサーバ200のハードウェア構成も、図2と同様であるが、ハードディスクにはサービス提供のためのサービス提供ウェブサーバプログラムが記録されている。

【0024】図3は、携帯情報端末100のハードウェア構成の一例である。携帯情報端末100は、CPU102、ディスプレイ104、スピーカ106、入力部108、RAM110、ROM112、インターネット300に接続するための通信回路114を備えている。CPU102は、携帯情報端末100全体を制御する。ROM112は、CPU102を動作させるためのプログラムや、この携帯情報端末100で実行することができ音声データ、画像データ等の他に、ウェブを閲覧するためのブラウザプログラムが記録されている。RAM110は、CPU102がデータ処理を行うための領域を提供する。入力部108の操作により生成される操作情報は、CPU102に入力され、CPU102が生成した画像情報及び音声情報は、ディスプレイ104、スピーカ106にそれぞれ出力される。

【0025】特許請求の範囲に記載した用語と実施形態との対応は以下の通りである。ユーザ端末は、図1の携帯情報端末100に対応し、認証装置は、図1の認証サーバ10に対応する。キー情報は、図4ステップS506で示すキーに対応する。認証用情報は、図6AステップS608で示す認証コードに対応する。

【0026】キー情報受信手段は、図4ステップS514で示すCPU102が行う処理に対応する。第1識別情報は、図6AステップS603で入力される第1識別情報に対応し、第2識別情報は、ステップS603で入力される第2識別情報に対応する。識別情報入力手段は、ステップS603で示すCPU102が行う処理に対応する。情報変更は、図6AステップS604で示すCPU102が行うハッシュ値の演算アルゴリズムが対応し、不可逆変更情報及び変更情報生成手段は、図6AステップS604で得られるハッシュ値が対応し、不可逆変更情報生成手段は、ステップS604で示すCPU102が行う処理に対応する。認証用情報生成手段は、図6AステップS608で示すCPU102が行う処理に対応し、認証用情報送信手段は、図5ステップS516で示すCPU102が行う処理に対応する。

【0027】識別情報記憶手段は、認証サーバ10のハードディスク20に記録された、図4Bに例示するユーザ管理データベース14が対応する。キー情報送信手段は、図4ステップS512で示すCPU16が行う処理に対応する。認証用情報受信手段は、図4ステップS518で示すCPU16が行う処理に対応する。キー情報取得手段は、図6BステップS654で示すCPU16が行う処理に対応する。第2識別情報取得手段は、図6BステップS658で示すCPU16が行う処理に対応する。確認用不可逆変更情報は、図6BステップS66

0で得られるハッシュ値が対応し、確認用不可逆変更情報生成手段は、ステップS660で示すCPU16が行う処理に対応する。ユーザ認証手段は、図6BステップS662で示すCPU16が行う処理に対応する。

【0028】キー部分情報は、図5ステップS508で得られる第1キー部分が対応する。キー情報記憶手段は、図4Aに例示するセッション管理データベース12が対応する。暗号解読手段は、図6BステップS656で示すCPU16が行う処理に対応する。

【0029】3. ユーザ認証処理の説明  
本システムのユーザ認証の概要を、図7を参照しながら説明する。本システムでは、ユーザ認証の際に、認証サーバ10によって任意に作成される“キー”と、携帯情報端末100によって入力される“第1識別情報”と、“第2識別情報”とを使用する。認証サーバ10は、システムに登録された各ユーザ毎に、あらかじめ第1識別情報と第2識別情報とを対応づけてデータベースに登録している。

【0030】認証サーバ10側では、キーを生成し（記号1）、これを携帯情報端末100に送信する（記号2）。携帯情報端末100側では、キーを受信して、キーと第2識別情報を含めた情報の不可逆変更情報（不可逆変更情報は、ハッシュ値とする）を演算し（記号3）、この不可逆変更情報に、キーと、第1識別情報とを付加したものを認証コードとして認証サーバ10に送信する（記号4）。

【0031】認証サーバ10側では、受信した認証コード中の第1識別情報に基づいてデータベースを参照し、対応する第2識別情報を取得する（記号5）。次に、この第2識別情報と、受信した認証コード中のキーとを含めた情報の不可逆変更情報を演算する（記号6）。そして、得られた不可逆変更情報と、受信した認証コード中の不可逆変更情報とを比較して（記号7）、両者が一致すれば、それは、最初に認証コードを送信した携帯情報端末100のユーザが、登録された第1識別情報と対応する第2識別情報を持つ正規のユーザであることになるので、ユーザ認証を完了する。

【0032】このように、本システムでは、第2識別情報が、任意のキーと合わせて不可逆変更情報とされているため、第三者に漏洩することなく、簡単なユーザ認証処理によって十分なセキュリティを確保することができる。さらに、本システムでは、以下に説明するように、第三者による情報の不正取得をより困難とするために、認証コードとして、キーの全部ではなく一部分を付加されたものを作成し、さらに、第1識別情報と、不可逆変更情報の部分を暗号化している。これらの処理の内容については、後述する。

【0033】以下、本発明の実施形態として、図1に示す携帯情報端末用ユーザ認証システムによるユーザ認証処理について説明する。ここでは、携帯情報端末100

のユーザが、Webサーバ200のサービスについての課金処理を受ける前提として認証サーバ10によるユーザ認証を受ける例を、図5、図6のフローチャートに基づいて説明する。

【0034】携帯情報端末100のCPU102は、図5、図6Aのフローチャートに従って認証コードの作成処理、送信処理等を行い、認証サーバ10のCPU16は、図5、図6Bのフローチャートに従ってキーの送信、ユーザ認証処理等を行う。

【0035】認証サーバ10のハードディスク20には、あらかじめユーザ管理データベース14が記録されている。ユーザ管理データベース14の構成の一例を、図4Bに示す。ユーザ管理データベース14には、Webサーバ200のサービスを利用することについての登録を受けている携帯情報端末100のユーザの情報が記録されており、それらの情報は、第1識別情報、第2識別情報、名前、住所、プロフィール等である。

【0036】携帯情報端末100のCPU102は、Webサーバ200の課金処理を受ける前提として、認証サーバ10にアクセスする（図5ステップS502）。認証サーバ10のCPU16は、アクセスがあるか否かを判断しており（ステップS504）、アクセスがあればキーを作成する（ステップS506）。キーは、固定長の乱数記号である。CPU16は、作成したキーを、第1キー部分と、第2キー部分に分割し（ステップS508）、セッション管理データベース12に登録する（ステップS510）。セッション管理データベース12の構造の一例を、図4Aに示す。キーは、第1キー部分のカラムと、第2キー部分のカラムに分割して記録され、各キーの有効期限もカラムに記録される。なお、CPU16は、ステップS506においてセッション管理データベース12を参照することにより、既に記録されているキーとは異なるものを作成するものになっている。

【0037】認証サーバ10のCPU16は、キーを携帯情報端末100に送信する（ステップS512）。携帯情報端末100のCPU102は、キーを受信するか否かを判断しており（ステップS514）、受信した場合には、認証コード作成処理（図6A）を行う。CPU102は、受信したキーを、第1キー部分と、第2キー部分に分割する（図6Aステップ602）。キーを分割する際のルールは、認証サーバ10における図5ステップS508におけるものと同じものである。CPU102は、ユーザの操作によって第1識別情報と第2識別情報の入力があるか否かを判断する（図6Aステップ603）。CPU102は、第1識別情報と第2識別情報の入力があったと判断すれば、“第2識別情報とキーとを合わせた記号列についての不可逆変更情報”を演算する（ステップS604）。CPU102は、得られた不可逆変更情報と第1識別情報とを合わせた記号列を暗号化する（ステップS606）。ここでの暗号化は、元の



記号列を、所定のアルゴリズムによって乱数化するようにしている。CPU102は、暗号化された不可逆変更情報と第1識別情報とに対して、第1キー部分を付加することによって、認証コードを作成する(ステップS608)。図6AステップS604、606、608において説明したように、認証コードは、第1キー部分、及び、第1識別情報と不可逆変更情報とを合わせた記号列を暗号化した部分と、によって構成されている。

【0038】携帯情報端末100のCPU102は、以上の認証コード作成処理を行った後、その認証コードを認証サーバ10に送信する(図5ステップS516)。認証サーバ10のCPU16は、認証コードを受信するか否かを判断しており(ステップS518)、受信したと判断すれば、認証処理(図6B)を行う。

【0039】認証サーバ10のCPU16は、認証コード中の第1キー部分を認識して、この第1キー部分が図4Aに例示するセッション管理データベース12に記録されているか否かを判断する(図6BステップS652)。CPU16は、第1キー部分がセッション管理データベース12に記録されていないと判断すれば、そのユーザ認証は“エラー”であると判断する(ステップS664)。ここで、“エラー”と判断する理由は、例えばそのユーザが、認証サーバ10にアクセスすることなく不正にキーを偽造した可能性があるか、あるいは、インターネット300上で送受信されるキーを不正に取得して、本システムで規定されるキーの分割についてのルール(図5ステップS602参照)に従うことなく認証コードを偽造した可能性があるために、第1キー部分がセッション管理データベース12に記録されていないことになるからである。

【0040】CPU16は、第1キー部分がセッション管理データベース12に記録されていると判断すれば、セッション管理データベース12に記録されているその第1キー部分に対応する第2キー部分を取得することによって、キー全体を取得する(ステップS654)。CPU16は、取得したキーをセッション管理データベース12から消去する(ステップS655)。CPU16は、認証コード中の、第1識別情報と不可逆変更情報とを合わせた記号列を暗号化した部分を認識して、これらの暗号を解く(ステップS656)。これにより、CPU16は、第1識別情報と、“第2識別情報とキーとを合わせた記号列についての不可逆変更情報”と、を取得する。

【0041】認証サーバ10のCPU16は、取得した第1識別情報に基づき、図4Bに例示するユーザ管理データベース14に記録されているその第1識別情報に対応する第2識別情報を取得する(ステップS658)。CPU16は、その取得した第2識別情報と、ステップS654で取得したキーとを合わせた記号列についての不可逆変更情報を演算する(ステップS660)。こ

での不可逆変更情報の演算は、図6AステップS604において携帯情報端末100のCPU102が行ったものと同一のものをを用いている。認証サーバ10のCPU16は、演算した、“第2識別情報とキーとを合わせた記号列についての不可逆変更情報”と、図5ステップS518で受信した認証コード中の、“第2識別情報とキーとを合わせた記号列についての不可逆変更情報”と、を比較して、両者が合致するか否かを判断する(図6BステップS662)。CPU16は、合致しないと判断すれば、そのユーザ認証は“エラー”であると判断する(ステップS664)。ここで、“エラー”と判断する理由は、例えばそのユーザが、図6AステップS603において、図4Bのユーザ管理データベース14に記録された正規の第2識別情報とは異なるものを入力したか、あるいは、そのユーザが、不正に他人の第1識別情報を取得した者であるために正規の第2識別情報とは異なる第2識別情報を入力していることになるために、両不可逆変更情報が合致しないということになるからである。

【0042】認証サーバ10のCPU16は、両不可逆変更情報が合致すると判断すれば、そのユーザ認証について“認証完了”であると判断する。

【0043】CPU16は、以上のユーザ認証処理を行った後、“認証完了”または“エラー”であるかを判断する(図5ステップS520)。CPU16は、携帯情報端末100に対して、“エラー”であればエラー情報を送信し(ステップS522)、“認証完了”であれば認証許可情報を送信する(ステップS524)。以上の処理により、ユーザ認証処理は終了する。

【0044】ユーザ認証がされた携帯情報端末100のユーザは、この後、Webサーバ200のサービスについての課金処理を受けることになる。

【0045】4. 本システムによる効果  
携帯情報端末用ユーザ認証システムでは、携帯情報端末100のCPU102は、第2識別情報に対する不可逆変更情報を演算している(図6AステップS604参照)。これにより、その不可逆変更情報単独では、不可逆変更情報の演算アルゴリズムが知られたとしても、第2識別情報が取得されたり再現されることがない。すなわち、例えばCPU102が認証コードを送信する際に(図5ステップS516参照)、第三者によって不可逆変更情報を不正に取得された場合でも、第2識別情報が取得されたり再現されることがない。したがって、本システムによれば認証システムは、ユーザ認証を安全かつ適切に行うことができる。

【0046】また、この第2識別情報は、認証サーバ10のCPU16が送信する任意のキーを含められて(図5ステップS506参照)、不可逆変更情報とされている。すなわち、同一の第2識別情報を用いても、携帯情報端末100のCPU102は、ユーザ認証を受け

るためにアクセスすることに、異なる不可逆変更情報を生成する。したがって、第三者にその不可逆変更情報を不正に取得されて場合でも、その不可逆変更情報別別のユーザ認証では無効なものになるので、ユーザ認証の信頼性が確保される。

【0047】携帯情報端末100のCPU102と、認証サーバ10のCPU16が行う不可逆変更情報の演算は、コンピュータによる簡単な演算によって行われる(図6AS604、S660参照)。したがって、携帯情報端末100または認証サーバ10として、低い演算能力しか持たない低スペックの機器を採用した場合であっても、ユーザ認証を安全かつ適切に行うことができる。

【0048】特に本システムは、ユーザ端末側に重い処理をさせる必要がないことから、パーソナルコンピュータ等に比べて低スペックのブラックボックス的な機器にも好適なものである。そのような機器においては、暗号化モジュールが外部に漏れる可能性が高くないから、認証コード作成処理のロジックが知られることも少ない。いずれにしても、本システムによるユーザ認証処理では第2識別情報が不可逆変更情報とされているため、たとえ図6Aに示す認証コード作成処理のロジックが知られたとしても、正規の第2識別情報と盗聴されていなければ、なりすまし等による不正なユーザ認証がされることはない。したがって、ユーザ端末に簡単な暗号化モジュールを搭載するだけで十分なセキュリティが確保できる。

【0049】認証サーバ10のCPU16は、認証コードに含まれる第1識別情報に基づいてユーザ管理データベース14を検索することにより第2識別情報を取得する(図6BステップS658)。したがって、CPU16は、図6BステップS660における不可逆変更情報の演算に必要となる第2識別情報を迅速に取得することができる。結果としてユーザ認証を迅速に行うことができる。

【0050】携帯情報端末100のCPU102は、認証コードの一部として、キー全体ではなく、第1キー部分を送信している(図6AS608参照)。これにより、例えば認証サーバ10のCPU16が携帯情報端末100にキーを送信する際に(図5ステップS512参照)、第三者によってキーを不正に取得された場合でも、どのような規則でキーの一部を第1キー部分としているかは特定されないため、第三者が第1キー部分を特定することは困難である。そして、認証サーバ10のCPU16は、受信した第1キー部分がセッション管理データベース12になければ、ユーザ認証を“エラー”とする(図6BステップS652、S664参照)。したがって、本システムでは、ユーザ認証をより安全かつ適切に行うことができる。

【0051】認証コードは、第1キー部分と、第1識別

情報と不可逆変更情報とを合わせた記号列を暗号化した部分とが含まれた後、携帯情報端末100のCPU102によって送信される(図6AステップS608参照)。したがって、例えばCPU102が認証コードを送信する際に、第三者によってこの認証コードを不正に取得された場合でも、第三者が第1識別情報と演算した不可逆変更情報とを特定することは困難である。したがって、本システムでは、ユーザ認証をより安全かつ適切に行うことができる。

【0052】5. その他の実施形態  
図5ステップS502において、本実施形態では、CPU102が認証サーバ10に直接アクセスするようにしているが、これに限られるものではない。その他の実施形態として、Webサーバ200のホームページ上に認証サーバ10のリンク情報を掲載するか、あるいは、Webサーバ200から認証サーバ10にリダイレクトを強制的にアクセスさせるようにしてもよい。

【0053】図5ステップS506において、本実施形態では、CPU16がセッション管理データベース12を参照することにより、既に記録されているキーとは異なるものを作成するようにしているが、これに限られるものではない。その他の実施形態として、作成した乱数に対して、さらに、識別用IDを自動添付して付加したものをキーとするようにしてもよい。

【0054】図5ステップS508において、本実施形態では、キーの分割のルールを一定のものとしているが、これに限られるものではない。その他の実施形態として、キーの分割のルールを変動するようにすることもできる。この場合、認証サーバ10と携帯情報端末100との間で、そのようなルールの変動の規則を一致させておく必要がある。

【0055】また、キーを分割するという処理ではなく、キーを2つ以上作成する処理としてもよい。この場合、2以上のキーの役割の関係(不可逆変更情報とされるキー、認証コードに付加されるキー等)をセッション管理データベース12に記録しておき、図6AステップS604において、携帯情報端末100のCPU102は、不可逆変更情報とするキーと、認証コードに付加するキーとを別のものとする。そして、認証サーバ10のCPU16は、認証コードに付加されたキーに基づいて、セッション管理データベース12を参照して不可逆変更情報とされているキーを取得するようにしてもよい。

【0056】なお、キーを分割することについては、上述したように、第三者によるキーや第1キー部分の特定を困難とするものの他、認証コードのデータ量を少なくして携帯情報端末100のCPU102の処理を軽くする利点があるが、このようなキーの分割処理を省略してもよい。この場合、図6AステップS608において、認証コードには、キー全体が付加され、図6Bステップ

S654において、認証サーバ10のCPU16は、セッション管理データベース12を検索することなくキーを取得することになる。

【0057】図6AステップS603において、本実施形態では、CPU102が、ユーザの操作に応じて第1識別情報と第2識別情報の入力があるかを判断することとしているが、これに限られるものではない。その他の実施形態として、CPU102は、携帯情報端末100に記録されている携帯情報端末100自体のマシンIDを自動送信することしたり、あるいは、ユーザの入力操作を必要とすることなく、携帯情報端末100のメモリや外部のメモリカード等に記録されている第1識別情報または第2識別情報、あるいは両方を自動送信することとしてもよい。

【0058】図6AステップS604において、本実施形態では、第2識別情報とキーを合わせた記号列について不可逆変更情報を演算することとしている。この不可逆変更情報の演算のアルゴリズムは、MD2、MD4、MD5等のハッシュ関数を用いてもよいし、ハッシュ関数以外の、不可逆な一方関数や、単に元情報を変更することによって元情報を再現できない情報とする手法を用いて演算してもよい。

【0059】また、ステップS604においては、CPU102は、“第2識別情報にキーを付加した記号列”の不可逆変更情報を演算することとしているが、これに限られるものではない。その他の実施形態として、“第2識別情報の記号列とキーの記号列”を、所定の規則によって組み合わせた記号列とした後に不可逆変更情報を演算するようにしてもよい。この場合、認証サーバ10のCPU16も、図6BステップS660において、その規則と同様の規則によって“第2識別情報とキーを組み合わせた記号列”の不可逆変更情報を演算することになる。

【0060】図6AステップS606の暗号化は、本実施形態では、元の記号列を、所定のアルゴリズムによって乱数とするようにしているが、これに限られるものではなくその他の暗号化アルゴリズムを採用してもよい。いずれにしても、本実施形態では、第2識別情報は不可逆変更情報とされているから、第三者によって第2識別情報が盗聴される可能性はほとんどない。したがって、ここでの暗号化アルゴリズムは、公開鍵暗号方式で利用されるRSA暗号系や楕円曲線暗号のようなセキュリティ機能が非常に高いものを用いることもできるが、一般的な携帯情報端末のような低スペックのCPUに重い処理をさせることを避けることを考慮すれば、簡単な暗号化アルゴリズムで、かつ、鍵がなくても解けるものが好ましい。

【0061】また、ステップS606においては、CPU102は、第1キー部分を暗号化しないこととしているが、これに限られず、第1キー部分も暗号化するよう

にしてもよい。

【0062】図6BステップS662では、本実施形態では、CPU16は、“第2識別情報とキーとを合わせた記号列についての不可逆変更情報”と、と比較して、両者が合致するか否かを判断することとしているが、これに限られるものではない。その他の実施形態として、CPU16は、携帯情報端末100側が送信する“第2識別情報とキーとを合わせた記号列についての不可逆変更情報”と、認証サーバ10側が演算する“第2識別情報とキーとを合わせた記号列についての不可逆変更情報”とを比較する際に、あらかじめ定められた規則に基づいて両者の一致性を判断するようにしてもよい。

【0063】本実施形態においては、ユーザ認証に用いる情報として、携帯情報端末100側から入力される、第1識別情報と第2識別情報の2つを用いることとしているが、これに限られるものではない。その他の実施形態として、3以上の情報を入力させるようにしてもよい。この場合、それらの情報は、認証サーバ10のユーザ管理データベース14にあらかじめ記録されることになる。その他、第1識別情報または、第2識別情報のうちいずれか一方のみを用いることとしてもよい。この場合、認証サーバ10のユーザ管理データベース14には、ユーザを特定する情報として第2識別情報のみを記録する。そして、認証サーバ10のCPU16は、図6Bの認証処理において、ステップS658の処理を行わずに、ユーザ管理データベース14にあらかじめ記録された全ての第2識別情報に対して、取得したキーを付加して総当りの不可逆変更情報を演算し、その不可逆変更情報の中に、受信した認証コード中の不可逆変更情報と合致するものがあれば、そのユーザ認証について“認証完了”であると判断するようにすればよい。

【0064】また、ユーザ端末側から送信する認証情報には、キー情報を付加しないようにしてもよい。この場合、認証装置からキー情報を送信する際、そのキー情報と、送信先であるユーザ端末の第1識別情報を対応づけて記憶しておけばよい。これにより、認証装置側は、受信した認証情報中の第1識別情報に基づいて、キー情報を取得することができる。

【0065】本実施形態の携帯情報端末用ユーザ認証システムでは、ユーザ端末として、携帯情報端末100を使用する例を示したが、これに限られるものではない。その他の実施形態として、ユーザ端末は、例えば、EZ Web (登録商標)、J-SKY Web (登録商標)、iモード (登録商標) のようなブラウザ搭載の携帯電話や、携帯ゲーム機、PDA、インターネット家電、インターネット対応時計、固定電話等にブラウザとモデムを搭載した機器等の、低スペックなインターネット端末であってもよい。また、TVショッピング等でユーザ認証が必要な場合に、デジタルTVと認証サーバとの間で本システムを利用することもできる。この場合、キー

は、放送電波等によって送信し、デジタルTV側の認証コードは、インターネット上に送信するようにすればよい。

【0066】なお、本実施形態では、携帯情報端末100のユーザの操作によって入力される情報を、それぞれ、“第1識別情報”及び“第2識別情報”としたが、第1識別情報として、例えば、無二の情報(ユニーク情報)であるユーザID、第2識別情報として、ユーザIDを正規なものとするための、例えば、パスワード等を採用すればよい。また、認証サーバ10側で作成される情報を、“キー”及び、それらが分割されたものを、“第1キー部分”、“第2キー部分”した。これらの情報については、実際のシステムの運営の際に便宜上、“ワンタイムキー”、及び分割されたそれぞれを、“キーID”、“ボディ部”という記号名を採用してもよい。

【0067】本実施形態では、CPU16の動作のためのプログラムや、CPU16のためのユーザ認証プログラムを、ハードディスク20、ROM112のそれぞれに記憶させているが、それらのプログラムは、プログラムが記憶されたCD-ROMから読み出してハードディスク等にインストールすればよい。また、CD-ROM以外に、フロッピー(登録商標)ディスク(FD)、ICカード等のプログラムをコンピュータ可読の記録媒体からインストールさせるようにしてもよい。さらに、通信回線を用いてプログラムをダウンロードすることもできる。また、CD-ROMからプログラムをインストールすることにより、CD-ROMに記憶させたプログラムを間接的にコンピュータに実行させるようにするのではなく、CD-ROMに記憶させたプログラ

ムを直接的に実行するようにしてもよい。

【0068】なお、コンピュータによって、実行可能なプログラムとしては、そのままのインストールだけで直接実行可能なものはもちろん、一旦他の形態等に变换が必要なもの(例えば、データ圧縮されているものを、解凍する等)、さらには、他のモジュール部分と組合して実行可能なものも含む。

【図面の簡単な説明】

【図1】携帯情報端末用ユーザ認証システムの装置構成を示す図である。

【図2】認証サーバ10のハードウェア構成の一例を示す図である。

【図3】携帯情報端末100のハードウェア構成の一例を示す図である。

【図4】図4Aは、セッション管理データベース12の構成の一例を示す図である。図4Bは、ユーザ管理データベース14の構成の一例を示す図である。

【図5】ユーザ認証処理のフローチャートである。

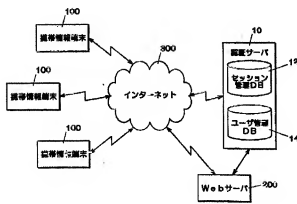
【図6】図6Aは、携帯情報端末100のCPU102による認証コード作成処理のフローチャートである。図6Bは、認証サーバ10のCPU16による認証処理のフローチャートである。

【図7】ユーザ認証処理の概要を示す図である。

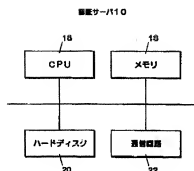
【符号の説明】

100・・・携帯情報端末  
200・・・Webサーバ  
10・・・認証サーバ  
12・・・セッション管理データベース  
14・・・ユーザ管理データベース  
300・・・インターネット

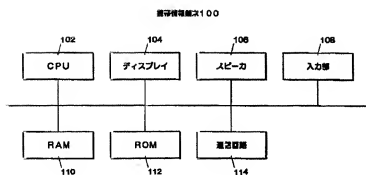
【図1】



【図2】



【図3】



【図4】

A

セッション管理D:

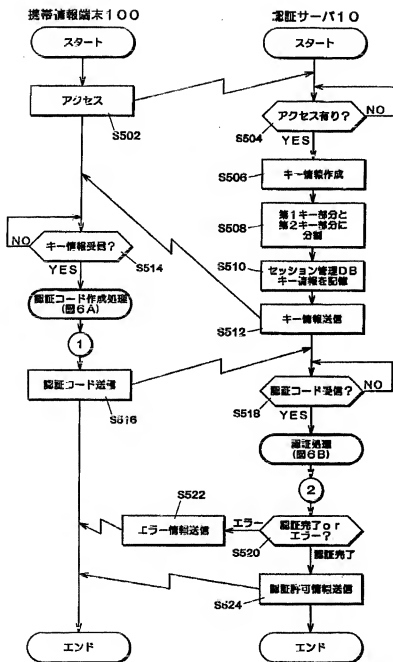
第1セッションID	第2セッションID	有効期限
0x6rm8or2o3aa	V1234	2001/1/24 09:21
0394u5Na0Fhe3TD	x5093	2001/1/26 10:08
...	...	...

B

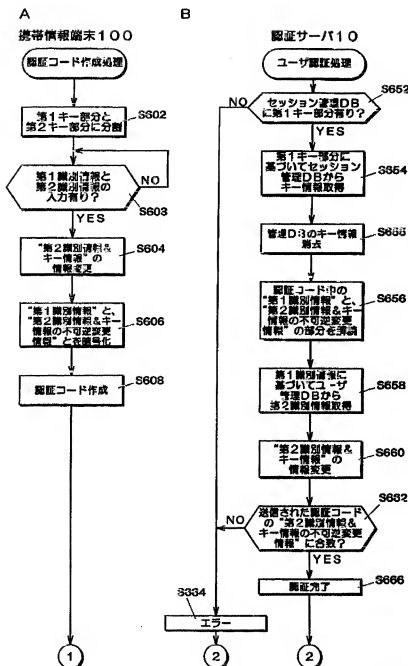
ユーザ管理DB

第1属性情報	第2属性情報	名前	性別	プロフィール
Ohta	hr89	Ohta	♂	...
Naka	mc3	Naka	...	...
...	...	...	...	...

【図5】



【図6】







( 7 2 ) 発 明 者 大 木 浩

滋 賀 県 八 日 市 市 蛇 溝 町 長 谷 野 1 1 6 6 - 6 京  
セラココミュニケーションシステム株式会社  
滋賀事業所内

( 7 2 ) 発 明 者 高 石 敦 哉

滋 賀 県 八 日 市 市 蛇 溝 町 長 谷 野 1 1 6 6 - 6 京  
セラココミュニケーションシステム株式会社  
滋賀事業所内

F ターム ( 参 考 ) 5B085 AE02 AE23 AE29 BG07

5J104 AA07 KA01 KA06 MA01 NA12

PA07 PA11